甲方合同编号：【　　】

乙方合同编号：【　　】

【长葛市城市管理局】与长葛市葛天智慧城市运营有限公司和河南移动【许昌】分公司关于【长葛数字城管机房托管及光纤租用项目】合作协议

甲方：【长葛市城市管理局】（盖章）

法定代表人/负责人：金智豪

住所：长葛市泰山路7号楼

授权代表签字：

乙方：（联合体牵头人）【 长葛市葛天智慧城市运营有限公司】（盖章）

法定代表人/负责人：张亚利

住所：长葛市东区葛天大道北侧3号楼14楼

授权代表签字：

（联合体成员）【 中国移动通信集团河南有限公司许昌分公司】（盖章）

法定代表人/负责人：李瑞杰

住所：许昌市八一路1786号

授权代表签字：

合同签订日期：【二〇二】年【 4 】月【 7 】日

根据《中华人民共和国民法典》、《中华人民共和国电信条例》及其他有关法律、法规的规定，在平等、自愿、公平、诚实、信用的基础上，双方就【长葛市城市管理局长葛数字城管机房托管及光纤租用项目 】有关事宜协商一致，达成合同如下：

第一条 合作内容

1.1 乙方在现有技术条件下、现有网络覆盖范围内，为甲方有偿提供【长葛市城市管理局长葛数字城管机房托管及光纤租用项目】集成及维保服务、【专线、移动云、5G SA 物联网卡、手机通信等】CT 业务服务。

1.2 乙方为甲方提供的具体服务内容、技术参数、验收标准及相关要求详见【附件 1：设备清单及技术规范】。当附件与合同正文不一致时，以合同正文为准，但涉及技术规范等专业性内容以附件中更为详细、准确的规定为准，前提是附件内容不与合同基本宗旨冲突；乙方为甲方提供的【CT 业务服务】除遵守本合同正文约定外，双方同时按照相应附件中的约定执行。

第二条 资费标准和支付方式

2.1 本合同项下甲方应当向乙方支付的服务费包括设备采购费、集成服务费、维保服务费、【专线、移动云、5G SA 物联网卡、手机通信等】CT 业务费用等。

2.2 本合同服务期限三年，甲方每年应当向乙方支付的服务费用共计【745000】元（大写：人民币柒拾肆万伍仟元整）。

2.3 合同项下所有款项由甲方向乙方以如下方式及比例支付：

【 支付方式为:合同签订后，甲方向乙方（即联合体牵头人）支付第一年费用金额的85%作为预付款，安装验收合格后 60 日历天内，甲方需一次性付清第一年费用并汇款到乙方（即联合体牵头人）账户。以后每年支付 745000 元。联合体牵头人每次在收到甲方支付的费用后，7 日内向联合体成员支付费用】

2.4 乙方银行账户信息

乙方名称：【长葛市葛天智慧城市运营有限公司 】

纳税人识别号：【91411082MA9GP7MB3C 】

户名：【 长葛市葛天智慧城市运营有限公司】

开户行：【郑州银行长葛支行 】

账号：【999156005430000522 】

地址：【长葛市东区葛天大道北侧 3 号楼 14 楼 】

联系电话：【 0374-2516197 】

任何一方如需改变上述账户信息（甲方名称和纳税人识别号不可改变），应在变更账户前十（10）日以书面通知另一方并征得对方同意。如一方未按本合同约定单独变更账户信息而使另一方遭受损失的，应予以赔偿。

2.5 结算周期内甲方向乙方支付的费用为：结算金额＝Σ（服务费±违约金）（说明：如甲方违约则使用“＋”，若乙方违约则使用“－”）。

2.6 结算方式采用【转账】（现金/转账等）的形式。

2.7 在甲方支付本合同项下的综合服务费之前，乙方应当向甲方开具相应金额的增值税【普通 】（/专用）发票。

第三条 服务内容及期限

3.1 服务内容

3.1.1 机房建设，甲方委托乙方将机房设备托管至乙方提供的专用机房，同时满足甲方需要的软硬件、1000MB 光纤、网络环境、视频环境、机房内部环境、电源(UBS)环境等。

3.1.2 机房建设的所有设备归甲方所有。服务合同结束后乙方须将机房建设的所有设备无条件运送到长葛市数字化城市管理中心。

3.1.3 乙方机房巡视，每周 1、3、5 进行常规巡视，做好巡视记录并及时排除故障。

3.1.4 提供 50 路室外网络高清视频图像信息和 80 部采集终端及信息采集车网络传输的无线服务。

3.1.5 提供人工坐席 30 台电脑 5 台打印机的维修服务。

3.2 具体服务需求

3.2.1 服务器及网络发生故障的响应时效，一般故障 4 小时；较大故障 2 个历日；特大故障至系统崩溃需上报甲方根据实际情况制定具体的维修历日。

3.2.2 乙方的光纤设备须满足与许昌市数字化城管平台的对接、12319 网络热线需求、长葛相关责任单位的网络传输、信息采集车、访问公安系统视频专网等无障碍对接。

3.2.3 核心机房建设内容：服务器、交换机、路由器、储存、防火墙、操作系统、防病毒系统等多台设备采购及托管。具体建设内容详见乙方响应文件。

3.2.4 本合同自双方签字盖章之日起生效，乙方应自合同生效之日起【40 】个日内完成平台集成及调测，达到交付验收标准。

3.2.5 自项目验收通过之日起乙方为甲方提供维保服务，维保期为【3】年。

第四条 验收

4.1 设备验收

4.1.1 甲方指定的地点及收货人:【长葛市、李瑞】。

4.1.2 开箱检验在乙方将货物运送至甲方指定交货地点后【3】日内进行，双方根据合同约定检查货物，检验后无任何问题的签署开箱检验合格证书。

4.2 验收标准

根据中华人民共和国国家和履约地相关质量标准、行业技术规范标准、采购文件的要求及乙方的响应承诺验收。

4.3 在乙方完成集成服务【7】个工作日内，双方应对项目成果进行验收，各项功能及指标符合要求的，由双方签署项目验收合格报告。

甲方自收到乙方提交的验收申请后【7】个工作日内未组织验收，且自乙方催告后【3】个工作日内仍未组织验收的，视为验收通过。

第五条 维保服务

乙方维保具体内容如下：

5.1 为保证系统正常运行所需的预防性维护、日常维护支持、网络调整支持、数据备份支持等工作。

5.2 提供每周【7】天每天【24】小时的技术支持服务。如果出现紧急技术问题，在甲方通过电话或传真通知乙方的情况下，乙方的工程师应在【1】小时内予以答复。如果甲方要求紧急处理，乙方应在收到甲方通知后的【1】小时内赶到现场，因自然灾害、交通管制等不可抗力导致的延误除外。当合同系统提供的业务中断时，乙方在提供远端服务的同时，须在收到甲方通知后【2】小时内赶到现场，因不可抗力致使乙方未按时到达现场的除外。

5.3 硬件设备发生损坏的，若在质保期内，设备维修或更换的成本由乙方承担（因甲方故意或使用不当导致设备损坏的除外）；软硬件质保期均为 3 年，若在质保期外，设备维修或更换的成本由甲方承担。

第六条 双方的权利与义务

6.1 甲方的权利和义务

6.1.1 在本合同有效期内，甲方有权要求乙方根据本合同约定向甲方提供相应的服务。

6.1.2 甲方同意乙方有权协同第三方从事部分合同约定的乙方服务工作。但是，乙方应对第三方的服务行为向甲方承担责任。

6.1.3 甲方应当根据其所使用的业务的要求向乙方提供真实有效的证件、资料和信息（包括但不限于甲方单位及相关授权人真实有效的营业执照、身份证、授权委托书等证件，以及白名单的相关资料等）。

6.1.4 甲方承诺并保证不利用乙方提供的集成维保服务进行任何违反国家政策、法律法规以及侵犯乙方或第三方合法权益的行为。否则，乙方有权立即停止向甲方提供所有产品和服务并解除本合同，一切后果由甲方承担。

6.1.5 甲方应本合同的约定，及时足额向乙方支付各项费用。

6.1.6 甲方如对乙方提供的产品和服务的费用产生异议，须于乙方向甲方通知相关费用之日起【15】日内向乙方提出，否则视为对费用的认可。

6.1.7 甲方应授权一名员工作为联系人，负责甲乙双方信息传递、服务实现、业务受理等方面的组织协调工作。甲方联系人需提供乙方所需的身份确认资料。甲方联系人如发生变更，需以书面形式通知乙方。

6.1.8 甲方开通使用乙方提供的相关产品时，需遵守对应的产品使用说明。甲方未按约定和相关要求使用产品的，相关责任由甲方承担。

6.1.9 甲方成为乙方集团客户后，如果乙方提供了服务账号；甲方应妥善保管乙方提供的服务账号和甲方设定的服务密码。服务账号和密码是甲方办理相关业务的凭证，凡使用服务密码进行的任何操作行为均被视为甲方或甲方授权行为。如因甲方服务账号和密码保管不

善等原因发生服务中断、业务变更、高额费用等情况，甲方应立即以书面形式通知乙方，乙方应采取可行的补救措施。甲方应当承担因账号和密码保管不善产生的费用。

6.1.10 如因甲方提供的相关资料不准确、不真实、不完整或变更后未通知乙方等原因，使乙方无法将服务提供给甲方，甲方承担由此造成的责任和后果。若甲方资料变更后未通知乙方导致乙方遭受损失（如额外成本支出、声誉损失等），甲方应承担相应赔偿责任。

6.1.11 未经乙方同意，甲方不得将乙方的软件、技术、设施等用于双方合作项目以外的其他用途，且不得向第三方透漏、转让。若甲方违反本条款，乙方有权要求甲方赔偿损失，终止协议。

6.1.12 未经乙方书面同意，甲方不得擅自使用中国移动的企业及品牌名称和标识、乙方的地方性品牌的名称和标识。否则，乙方有权解除合同并要求甲方赔偿损失。

6.2 乙方的权利和义务

6.2.1 乙方从事系统集成、维护等工作，需由乙方人员携带相关证件及单位证明，与甲方相关部门联系并办理相关手续，甲方应及时提供相关配合。

6.2.2 乙方进行检修线路、设备搬迁、工程割接、网络及软件升级或其他网络设备进行调试、维护工作，或因其他可预见性的原因可能影响甲方使用本合同约定服务的，应提前通知甲方，甲方应给予必要的配合。

6.2.3 乙方受理甲方的故障申报，应及时安排故障处理。乙方按维护及业务规程的有关规定，为甲方提供优质服务。

6.2.4 在合同有效期内，乙方有责任按照国家标准负责系统的日常运行维护工作。保障系统的正常运行，如发生故障，及时响应。

6.2.5 乙方有权根据本合同约定要求甲方及时足额支付各项费用。

6.2.6 乙方应对其所委托的代为向甲方提供本合同项下服务的第三方的服务行为向甲方承担责任，包括保证其提供的服务质量符合本合同约定，并对其服务瑕疵向甲方承担违约责任。

第七条　保密条款

7.1“保密信息”是指本协议拥有信息的一方（“提供方”）根据本协议向另一方（“接受方”）提供的信息，或接受方在本协议履行过程中从提供方处获知的信息。保密信息包括但不限于：技术方案、客户数据、技术信息、商业信息、商业秘密、文件、程序、计划、技术、图表、模型、参数、数据、标准、专有技术、业务或业务运作方法和其他保密信息，本协议的条款和与本协议有关的其他信息，本协议履行过程中形成的所有信息、数据、资料、意见、建议等。

7.2 保密信息只能由接受方及其人员为本协议目的而使用。除非本协议另有约定，对于提供方提供的任何保密信息，未经提供方事先书面同意，接受方及其知悉保密信息的有关人员均不得直接或间接地以任何方式提供或披露给任何第三方。甲方理解并同意，乙方及其关

联公司可通过业务受理系统登记、纸质档案，通过网络接收、读取并记录等方式，以提供电信服务为目的，在业务活动中收集、使用甲方提供的和甲方使用服务过程中形成的信息。乙方有权依法对包含甲方在内的整体用户数据进行分析并加以利用包括不限于匿名化处理后的统计分析等。未经甲方同意，乙方不向除乙方关联公司外的第三方提供甲方信息。乙方关联公司，是指中国移动通信集团公司及其在中华人民共和国境内直接或间接控股的主营通信业务的公司，以及上述公司的合法继承公司。

7.3 双方不得向任何人透露用户的信息、资料以及交易记录，除国家法律、行政法规另有规定外，双方均有权拒绝除用户本人以外的任何单位或个人的查询；同时，双方承诺采取不低于国家标准的技术措施保护数据安全，不得将数据存储于境外，双方应尽合理努力将电子支付交易数据以安全方式保存，并防止其在公共、私人或内部网络上传输时被擅自查看或非法截取。

7.4 接受方的律师、会计师、承包商和顾问为提供专业协助而需要了解保密信息时，接受方可向其披露保密信息，但是，其应要求上述人员签订保密协议或按照有关职业道德标准履行保密义务。接受方应向提供方承担因己方聘请的上述专业顾问违反保密约定而给提供方造成的任何损失。

7.5 如相关政府部门或监管机构要求接受方披露任何保密信息，接受方可在该政府部门或机构要求的范围内做出披露而无需承担本协议项下的保密责任。但前提是，该接受方应立即将需披露的信息书面通知提供方，以便提供方采取必要的保护措施，且该等通知应尽可能在信息披露前做出，并且接受方应尽商业上合理的努力确保该等被披露的信息获得有关政府机关或机构的保密待遇。保密信息不包括以下任何信息：（1）非因违反本协议所致，已进入公众领域的信息；（2）在提供方依据本协议做出披露前，接受方已合法拥有的信息；（3）接受方从有权披露的第三方获得的信息；及（4）接受方独立开发的信息，未使用任何保密信息。

7.6 双方应严格遵守保密条款之约定，严格履行保密义务，直至有关保密信息合法公开之时止。本协议或其任何条款的终止、中止、失效、无效均不影响本保密条款的有效性及对甲乙双方的约束力。

7.7 由于保密信息接受方未履行保密义务给提供方造成损失的，接受方应当赔偿由此给提供方造成的损失。

7.8 在任何情形下，本合同约定的保密义务应永久持续有效。

第八条　违约责任

8.1 甲方未按照本合同约定的期限支付合同款项的，从逾期的次日起计算违约金，每滞后 1 天支付未缴金额的【 1‰】。违约金总额超过合同金额的【20%】时，乙方有权解除本合同，并保留进一步追偿的权利。乙方解除合同后进一步追偿的范围包括但不限于未支付的款项、因甲方违约导致的乙方实际损失（如资金占用损失、为履行合同支出的额外费用等）

及实现债权的费用（如律师费、诉讼费等）。

8.2 因乙方原因导致乙方未按照本合同约定时间完成项目的，每逾期一天应向甲方支付合同金额 1‰的违约金。

8.3 乙方在进行网络调整和维护时需要短时间中断服务，或者由于 Internet 上骨干网通路的阻塞造成甲方服务器访问速度下降，甲方认同属于正常情况，不视为乙方违约。

8.4 下列情况下乙方有权单方终止本合同，并停止向甲方提供服务。由此给甲方造成的损失，乙方不承担责任，并有权要求甲方承担违约和赔偿责任：

（1）甲方（包括联系人）提供虚假证照的；

（2）甲方利用乙方提供的产品和服务实施违反国家法律、法规和政策的活动；

（3）甲方利用乙方提供的产品和服务从事其他不当用途或侵犯第三方的合法权利；

（4）乙方根据国家有关部门的要求停止为甲方提供相关服务。

8.5 乙方仅对因其过错给甲方造成的直接损害结果（如修复费用、合理停机损失）承担赔偿责任，且不包括第三方提出的索赔要求、数据丢失或损坏的损失，不包括甲方预期收益、商誉损失、经营损失等一切间接损失。无论何种情况，乙方对本协议项下的违约赔偿总额不超过本协议项下已支付的服务费用的总和。

8.6 如甲方未按本合同约定或国家法律法规规定及时办理相关备案或审批手续，因此产生的一切责任和后果均由甲方承担。根据国家法律法规、通信管理部门的规定或通知，乙方有权中断、终止为甲方提供本协议项下的全部或部分业务，且无需承担任何违约责任。

8.7 乙方对因其过错给甲方造成的直接损害结果承担赔偿责任，包括数据丢失或损坏等损失。如出现差错没有产生不良后果，出现一次甲方提出警告，乙方应实时整改，出现两次，甲方将按照当期合同金额 2%作为罚款，如果一年内出现三次(不含三次)上述差错，甲方将按当期合同金额 5%作为罚款。

8.7.1 服务期内乙方出现差错并对甲方工作产生影响的，每次按当期合同金额 5%作为罚款。

8.7.2 服务期内乙方出现重大差错，导致系统崩溃，数据丢失，乙方负责恢复数据的一切费用，甲方将按当期合同金额 50%作为罚款。如不能恢复，必须无条件重建，甲方将按当期合同全款作为罚款。

8.7.3 监控图像信息的上传，必须保证达到 100%的完好率，如果出现完好率低于 100%时，必须在 6 小时内解决并恢复图像传送，否则，甲方将按当期合同金额 1%作为罚款。

第九条　不可抗力及免责条款

9.1 本合同所指不可抗力，是指不能预见、不能避免并不能克服的客观情况。

9.2 由于不可抗力事件，致使一方在履行其在本合同项下的义务过程中遇到障碍或延误，不能按约定的条款全部或部分履行其义务的，遇到不可抗力事件的一方（“受阻方”），只要满足下列所有条件，不应视为违反本合同：（1）受阻方不能全部或部分履行其义务，是

由于不可抗力事件直接造成的，且在不可抗力发生前受阻方不存在迟延履行相关义务的情形；（2）受阻方已尽最大努力履行其义务并减少由于不可抗力事件给另一方造成的损失；（3）不可抗力事件发生时，受阻方立即通知了对方，并在不可抗力事件发生后的十五(15)天内提供有关该事件的书面说明，书面说明中应包括对延迟履行或部分履行本合同的原因说明。

9.3 不可抗力事件终止或被排除后，受阻方应继续履行本合同，并应尽快通知另一方。受阻方应可延长履行义务的时间，延长期应相当于不可抗力事件实际造成延误的时间。

9.4 如果不可抗力事件的影响持续达三十（30）日或以上时，双方应根据该事件对本合同履行的影响程度协商对本合同的修改或终止。如在一方发出协商书面通知之日起十（10）日内双方无法就此达成一致，任何一方均有权解除本合同而无需承担违约责任。

9.5 乙方对下述事项不承担责任：（1）第三方对甲方提出的索赔要求；（2）甲方的记录或数据的丢失或损坏；（3）甲方的经营损失等一切间接损失。

9.6 如因乙方难以避免、难以排除的技术或网络故障或第三方原因造成甲方无法使用本协议项下服务的，不视为乙方违约，但乙方应尽合理努力争取在最短时间内解决，对此双方无异议。鉴于计算机、移动通信网络及互联网的特殊性，因黑客、病毒、电信部门技术调整和骨干线路中断等引起的事件，在乙方能够出具相关合理证明材料的情况下，甲方亦认同不属于乙方违约。

第十条 通知与送达

10.1 根据本合同需要发出的全部通知，均须采取书面形式，对本合同效力产生影响的、或解决合同争议时的通知或函件，必须采用专人递送或者特快专递方式送达，上述书面通知均须标明合同对方为收件人。

10.2 上述书面通知按对方在本合同通知与送达条款中所列的地址发出，任何一方未按照本合同约定的送达方式送达的，视为未履行通知送达义务。如双方中任何一方的地址有变更时，须在变更前十日以书面形式通知对方，因迟延通知而造成的损失，由延迟通知方承担责任。

10.3 双方将按如下约定确定通知送达完成时间：

10.3.1 以专人递送的，接收人签收之日视为送达；

10.3.2 以特快专递形式发出的，发往本市内的，发出后第【3】日视为送达。发往国内其他地区的，发出后第【5】日视为送达；

10.3.3 以电子邮箱形式发出的，到达接收人电子邮箱所在系统之时视为送达；

10.4 合同各方均明知：因各方提供或者确认的通信地址和联系方式不准确、 或者通信地址变更后未及时依程序告知对方和司法机关、或者当事人和指定接收人拒绝签收等原因，导致商业信函、诉讼文书等未能被当事人实际接收，以专人递送的，送达至通知与送达条款约定的地址之日即视为送达之日；以特快专递形式发出的，按照通知与送达条款约定的时间确定送达之日。

10.5 各方地址与联系方式如下：

甲方：【 长葛市城市管理局 】

地址：【 长葛市泰山路 7 号楼 】

电话：【 15937423403 】

联系人：【 李瑞 】

电子邮件：【 15937423403@139.com 】

乙方：【长葛市葛天智慧城市运营有限公司】

地址：【 河南省许昌市长葛市东区葛天大道北侧 3 号楼 14 楼 】

电话：【 18837452666 】

联系人：【 李迪 】

电子邮件：【 18837452666@139.com 】

第十一条 争议解决

11.1 本合同的成立、有效性、解释、履行、签署、修订和终止以及争议的解决均应适用中华人民共和国法律。

11.2 如果任何争议或权利要求起因于本合同或与本合同有关或与本合同的解释、违约、终止或效力有关，都应由双方通过友好协商解决。协商应在一方向另一方送达关于协商的书面要求后立即开始。

11.3 如果在一方提出协商要求后的十(10)天内，双方通过协商不能解决争议，则双方同意向乙方住所地人民法院提起诉讼。

11.4 诉讼进行过程中，除双方有争议的部分外，本合同其他部分仍然有效，双方应继续履行。本合同全部或部分无效的，争议解决条款依然有效。

第十二条 其他约定

12.1 本合同一式【陆】份，甲方、联合体成员各方各持【贰】份，具有同等法律效力。

12.2 对于合同未尽事宜、双方可签订补充合同对本合同中的问题做出补充、说明、解释。本合同的补充合同作为本合同不可分割的一部分，与本合同具有同等的法律效力。

12.3 本协议附件作为本协议的一部分，与本协议具有同等法律效力。

12.4 在本协议有效期内，双方可以通过友好协商，对本协议相应条款进行变更或者解除本协议。任何一方欲变更或解除本协议，应提前 30 日向另一方提交书面说明。单方面解除协议的一方，应对另一方因此遭受的损失承担全部赔偿责任。

第十三条 本合同附件

附件 1：技术规范书

附件 2：网络与信息安全承诺书

（以下无正文）

附件 1：技术规范书

1．核心机房配置

序号	名 称	技术参数	单 位	数 量
1	数据库服务器	1.机型:2U 机架式高密度服务器，含导轨 ★2.CPU 类型：配置≥2 颗 Intel Xeon Silver 4316 20C 2.30GHz 30MB 150W； 3.内存：128GB DDR4 ECC REG RDIMM 内存，≥32 个内存插槽； 4.硬盘：3 块 2.5" 2.4T 10000RPM SAS 硬盘； 5.RAID 卡：12Gb 3108 8i Raid0 1 5 6 10 50 60 1GB 缓存 半高； 6.网卡：配置 2 个千兆电口以太网，独立 IPMI 管理接口； 7.HBA 卡：16Gb/s 双端口多模 PCIe x8 半高/全高(含光模块) 8.电源：≥800W 白金 1+1 冗余电源; ★9. 提供边缘安全云主机深度安全防护系统软件，支持 Windows、Linux 系统，含介质； ★10.数据保护：支持异构存储镜像的读写（Read/Write sequence & parallel）；支持快照在生产中心发起，自动传递到后期容灾中心的 DSP 中，使两端快照点数据一致；数据库模块服务：支持跨平台数据库；含跨平台数据库比对模块授权，提供数据库诊断服务，需定期出具跨平台数据库运维状态分析报告；通过可视化剖析关键的数据库度量指标、关联资源的使用到特定的查询语句，以及帮助可视化调优复杂的 SQL 语句；	套	2
2	应用服务器	1.机型:2U 机架式高密度服务器，含导轨 ★2.CPU 类型：配置≥2 颗 Intel Xeon Silver 4314 16C 2.40GHz 24MB 135W； 3.内存：128GB DDR4 ECC REG RDIMM 内存，≥32 个内存插槽； 4.硬盘：3 块 2.5" 2.4T 10000RPM SAS 硬盘； 5.RAID 卡：12Gb 3108 8i Raid0 1 5 6 10 50 60 1GB 缓存 半高； 6.网卡：配置 2 个千兆电口以太网，独立 IPMI 管理接口； 7.HBA 卡：16Gb/s 双端口多模 PCIe x8 半高/全高(含光模块) 8.电源：≥800W 白金 1+1 冗余电源; ★9. 提供边缘安全云主机深度安全防护系统软件，支持 Windows、Linux 系统，含介质； ★10.数据保护：支持异构存储镜像的读写（Read/Write sequence & parallel）；支持快照在生产中心发起，自动传递到后期容灾中心的 DSP 中，使两端快照点数据一致；数据库模块服务：支持跨平台数据库；含跨平台数据库比对模块授权，提供数据库诊断服务，需定期出具跨平台数据库运维状态分析报告；通过可视化剖析关键的数据库度量指标、关联资源的使用到特定的查询语句，以及帮助可视化调优复杂的 SQL 语句；	套	4
3	光纤交换机	24 端口交换机，24 端口激活，含 24 个 16Gb 短波多模 SFP，含 Web tools、Zoning 软件授权,EGM 软件授权，含级联许可，单电源，含导轨	套	1
4	数据存储	★1. 采用多活控制器结构，本次配置≥2 个控制器；每控制器采用≥1 颗 64 位处理器，处理器主频≥1.9GHz， 每处理器核心数≥6；CPU 支持超线程，若不支持超线程，则必须满足 CPU 同等物理核数要求; 2.高速缓存容量：配置控制器内存、缓存总容量≥128GB，每双控最大可扩展至 2TB (若配备独立文件引擎或模块，则不计入引擎或模块的内存、缓存。此内存、缓存非 SSD 或 PCI-E 接口闪存卡，且必须为读写双向内存）； ★3. 访问协议：配置 FC-SAN（FCP）、NAS（NFS\CIFS）、IP-SAN（iSCSI）、FTP 协议；SAN 控制器及 NAS 控制器为 冗余配置（皆为多控）；	套	1

		★4.NAS 支持：必须采用无 NAS 机头架构，无需额外 NAS 引擎和控制器，在单一控制器中同时支持 SAN 及 NAS； 5.配置磁盘容量：配置 SAS 磁盘数量≥8 块 2.5" 2.4T 10000RPM SAS HDD，≥8 块 3.5" 16T 7200RPM SAS HDD； ★6.SSD 缓存：配置 SSD 缓存功能，以提高存储 I/O 性能，且必须为读写双向加速，本次配置≥2 块 960G 企业级 SAS 接口 SSD 硬盘。 7.磁盘保护方式：必须支持 RAID 0，1，5，6，10、以及三块校验盘的 RAID 模式，支持同一 RAID 组中同时拔出任意 3 块硬盘业务不中断数据不丢失，在同一套系统内支持这些 RAID 方式的混合使用； ★8.主机接口：配置≥4 个 16Gb FC 主机接口(含光模块)+4 个 1Gb/s（电口）主机接口 9.后端磁盘箱接口：控制器（双控）配置≥4 个 12Gb/s SAS 接口； 10.系统管理：要求提供统一管理软件界面，可以同时管理 FC-SAN、IP-SAN 和 NAS；提供图形界面的系统性能监控 工具，可以实时监控存储系统的 CPU、吞吐量、各个协议的 IOPS、访问延迟等信息； 11.数据快照：配置数据快照功能许可，配置不低于本次配置容量的 License，支持≥4096 个快照，创建 4096 个 快照用时小于 16 分钟； 12.存储池功能：单一磁盘池可同时部署 SAN 及 NAS，无需为 SAN 及 NAS 分别建立磁盘池； 13.存储资源管理能力：单卷最大容量≥16PB；单存储池最大容量≥1EB；单个存储池最大支持≥1024 个卷，创建 1024 个卷用时小于 5 分钟； 14.数据修复与磁盘校验：配置数据修复与磁盘校验功能许可，raid-z3 拔盘前和拔三块硬盘后数据恢复过程中数 据的 IO 速率比相差小于 2000 次/s； 15.压缩：配置在线数据压缩功能许可，在线数据压缩（块级），可同时用于 SAN 及 NAS，并提供不少于 10 种压缩 算法，单个压缩一次可节省的空间达 30%以上，以提高存储使用效率； ★16.数据一致性检测：从主机端口到硬盘全路径支持基于硬件的并符合业界标准的 T10-PI 数据一致性检测，保障数据的一致性； 17. 云计算软件兼容性：兼容 Vmware、OpenStack、Kubernetes，银河麒麟云等云计算平台；支持不少于一家云厂商兼容性互相认证，并提供云厂商兼容性认证证书；必须提供 OpenStack Cinder 及 Man illa 驱动，以及 KubernetesCSI 驱动；		

5	核心交换机	1. 10/100/1000M 电接口 48 个，万兆光接口 6 个，冗余交流电源输入，采用前后直通风风道设计。 2. 交换容量 2.1Tbps,包转发率 1420Mpps 3. 支持 4K 个 VLAN，支持基于 MAC、IP 子网的 VLAN、支持 protocol vlan、支持 private valn、支持 voice vlan、支持 guest vlan，QINQ 等；多对一的端口镜像，远程端口镜像 RSPAN，流镜像。 4. 支持 G.8032 协议，实现 ms 级业务倒换，支持汇聚口路由组功能。 5. 支持 DHCP Server，静态路由、RIP、OSPF、BGP 和 RIPng、OSPFv3、BGP4+等动态路由协议；支持 BFD for VRRP/Static/RIP/OSPF 等,支持 MPLS MCE。 6. 支持 Local 认证，Radius，Tacacs+，AAA、802.1x 认证 7. 支持横向虚拟化功能，支持分布式设备管理、分布式链路聚合，统一路由管理。可以实现 16 台硬件设备之间的虚拟化部署，支持多虚一。 8. 设备支持 M-LAG 功能，支持跨设备链路聚合下双主检测功能。 9. 支持二层 VXLAN 网关，支持终端脆弱性扫描，支持纵向虚拟化。 10. 支持 ZTP,可实现零配置，零 IP 开局，支持能效以太网 11. 设备系统经过漏洞扫描软件测试，不存在高危漏洞 12. 支持 Telnet、Console、SNMP 等管理方式	台	2
6	接入交换机	1. 千兆电接口 48 个，SFP 千兆光口 4 个，固化双电源。 2. 交换容量 256Gbps，包转发率 95Mpps。 3. 支持 VLAN 划分，支持 4094 个 VLAN 4. 支持 STP/RSTP/MSTP 等生成树协议，可以避免网络出现环路 5. 支持 DHCP SERVER,支持静态路由、RIPV1/V2 动态路由 6. 支持 CPU 保护功能，如 ICMP Flood 拦截、SYN Flood 攻击拦截等，CPU 根据不同协议进行限速保护。 7. 支持 SNMP、TELNET、CONSOLE、SSH 和 WEB 管理等方式管理	套	4
7	边界协同处置系统	1. 标准机架式结构，冗余电源，标准配置 12 个 10/100/1000M 自适应电口、6 个千兆 SFP 光接口和 2 个万兆 SFP+光接口,1 个 Console 口，另外含有 2 个扩展插槽；含 3000 个 IPsecVPN 并发隧道数和 300 个 SSLVPN 并发用户数；含 3 年硬件维保和全功能规则库升级服务。 2. 支持代码注入、跨站脚本、输入验证、危险函数、代码质量、API 误用、密码管理、异常处理等常见安全缺陷问题的检测，二级缺陷类型不低于 2000 个； 3. ★支持对 web 业务系统进行源代码合规分析审计能力； 4. ★拥有自主知识产权的具有独立运营的漏洞响应平台； 5. 支持文件目录防护功能，通过对用户账号进行认证，对网站内容的修改行为进行合法性控制； 6. 支持与国家位置信息结合设置安全策略，识别流量发起的国家或地区的位置信息，根据流量发起的国家或地区的访问位置信息实现对不同区域访问的差异化控制； 7. ★支持通过扫描任务的方式检测目录中存在的恶意 Webshell。支持客户端自动识别 Web 应用所在 Web 目录进行扫描，也支持手动指定 Webshell 扫描目录。支持设置 Webshell 扫描文件类型，预置常见 Webshell 文件后缀； 8. ★支持借助主机 RASP 插件、主机 WAF 插件增强 Webshell 的实时监测能力，支持额外获取 Webshell 植入时的 HTTP 信息，包括方法、user-agent、url、域名等信息； 9. ★产品至少通过 3 家以上专业测评机构的安全检测。	套	2

8	网络监测预警系统	1. 标准机架式结构，有液晶面板，4TB 硬盘，标准配置千兆 6 个 10/100/1000M 自适应电口，4 个千兆 SFP 光口，2 个 40G QSFP 光口，2 个扩展插槽，2 组 bypass，1 个 Console 口，2 个 USB 接口。 2. 可实现基于 IP 地址、服务端口、IP 协议、物理端口、DSCP 值、IP 优先级、TOS 值、TTL 值、ICMP 类型、分片状态、TCP 状态、时间等安全策略的状态包过滤，支持源地址、目的地址的取反操作； 3. 支持 C&C 域名、DGA 域名、Sinkhole 域名的检测告警；支持挖矿域名检测，包括但不限于 MSASCMiner 挖矿病毒、SoulemanMiner 挖矿病毒 MoyuMiner 挖矿病毒、SkidMap 挖矿病毒、MadoMiner 挖矿病毒等； 4. 支持 DNS 隐蔽通道、DGA 规则、IDN 域名、FastFlux、DNS 反射放大攻击、可疑心跳域名、环路地址、可疑动态域名、DNS 重绑定等检测告警； 5. ★拥有自主知识产权的具有独立运营的威胁情报中心。	套	1
9	大模型数据共享交换平台	1. 硬件及性能：2U 机箱，冗余电源；接口：标准配置 12 个 10/100/1000M 自适应电口、8 个千兆 SFP 光接口,4 个万兆 SFP+光口，2 个扩展插槽，1 个 Console 口，2 个 USB 口； 2. 支持文件制定文件前缀、后缀、文件名暂缓传输，同时具备文件未传输完成时，增加文件指定前缀、后缀，传输完成以后自动删除该前后缀，以此来判断文件完整性； 3. 可通过自动、手动的任务设置，对局域网内服务器的服务器进行扫描（支持 ARP、Ping、Nmap 扫描方式，并支持离线分析），并自动获取服务器相关信息，包括 MAC 地址、设备类型、未知主机 IP、操作系统、发现方式、首次发现时间等信息； 4. 可对服务器的软件漏洞进行综合扫描，并可对扫描方式、扫描周期进行设置，并以报告的形式展示软件漏洞扫描结果，包括：问题机器 TOP5、影响最多漏洞 TOP5、漏洞发现趋势等； 5. 支持可网管型交换机信息的图形化展示，通过面板的形式详尽展现了交换机型号信息、交换机的端口数、各接口状态以及各接口下联的终端详细信息，方便管理员掌握全网网络设备信息； 6. 能准确感知终端的上线离线事件，详细记录了终端的上线时间，上线位置，离线时间等信息，方便管理员及时了解网络终端状况； 7. ★增值服务：引入基于行为分析和机器学习的智能检测技术，建立行为基线，检测异常行为，配合甲方完成大模型安全建模和分析服务。	套	1
10	应用能力服务系统	1. 标准机架式结构，1TB 硬盘，标准配置千兆 6 个 10/100/1000M 自适应电口，4 个千兆 SFP 光口，4 个万兆 SFP+光口插槽，1 个 Console 口，2 个 USB 口，2 个扩展插槽。 2. 支持通过 Vcenter 自动获取虚拟机状态，并将流量根据配置的负载均衡算法自动分配到各虚拟机。支持虚拟机管理，可监控虚拟机 cpu 占用率，内存占用率，健康状况，连接数等的状态；并根据以上条件对虚拟机进行关闭，挂起，重启，开启等操作； 3. 通过应用层代理，可解析客户端请求内容，并根据客户端请求头域做内容分发，将访问不同内容的请求代理到相应服务器上；并将响应数据代理到对应客户端。例如对图片类、文字类的请求，分别转发到对应的图片、文字服务器，支持基于 Cookie、User-Agent、URL、HTTP 头的分担模式； 4. 支持对认证源进行管理，可进行认证源添加，默认支持本地认证；可对接 AD 域认证、LDAP 认证、PKI 证书认证、企业微信认证、飞书认证、扫码认证(奇安信 ID 扫码)，邮箱认证、CAS 认证，短信网关、蓝信认证、钉钉认证，飞天 OTP 令牌等，	套	1

		支持创建多个认证源； 5. 支持全网视角的终端资产统一清点，清点信息包括操作系统、应用软件、监听端口和主机账户，其中操作系统、应用软件和监听端口支持从资产和终端两个视角进行统计和展示； 6. 支持资产自助登记、自助分组功能，支持硬盘序列号收集、支持 SN 号收集；支持按终端维度展示终端的硬件、软件、操作系统、网络、进程等信息； 7. ★增值服务：配合甲方完成安全防范管控梳理工作，包括安全监控视频、重大设备灾害防治、监测感知数据信息、风险评估报告、风险监测预警信息等。		
11	实战化威胁监测系统	1. 硬件及性能：标准机架式结构，标准配置 4 个 10/100/1000M 自适应电，2 个万兆 SFP+光口，内置 4TB 硬盘，2 个扩展插槽； 2. 支持常用的网络协议流量，类型包括 HTTP、FTP、POP3、SMTP、DNS、SNMP、ARP 等，提供数据采集策略配置，提供基于源地址、目的地址、应用、流量采样比、时间进行选择数据采集对象，可以针对采集对象进行网络流量数据采集和威胁监测数据采集，网络流量数据采集提供自定义流量载荷字节数； 3. 提供对主机设备、网络设备、安全设备、应用系统设备等的漏洞信息进行监测，提供导入第三方漏洞扫描报告，系统主流扫描器漏扫报告的解析识别和导入管理，提供人工漏洞报告导入，用户根据系统自带的导入模板进行漏洞信息的导入； 4. 提供信息预处理功能，可以通过简捷配置相关解析规则、过滤规则、富化规则、日志类型，来达到归一化、过滤、丰富、分类日志信息的目的； 5. 提供通过工单处理流程对告警事件及脆弱性事件进行跟踪，提供将安全事件以工单形式通过邮件、短信、消息中心通知责任人，以及时对事件进行处置； 6. 提供对最近 1 天、7 天、30 天等维度以仪表视图的方式展示新增工单量、处置中工单量、处置工单、工单处置周期分布、新增工单变化趋势、处置中工单优先级分布、新增工单状态分布、责任人处置工单排行、责任人新增工单排行、最近的工单等统计数据； 7. ★增值服务：配合甲方完成采集数据基础工作，主要包括安全监测数据、视频图像数据、重大设备监测数据；	套	1
12	实战化威胁分析系统	1. 为用户提供 7×24H 全天候的安全威胁监测服务，以威胁发现为基础、以分析处置为核心、以发现隐患为关键、以推动安全运营能力提升为目标，帮助用户进一步提升检测、监测、分析、预警、响应、处置的安全运营能力，协助用户完成威胁事件的闭环工作，通过运营驱动安全体系提升， 2. 资产识别：支持识别网络交换设备、网络安全设备、物联网设备、服务器设备、存储设备、办公外设、大数据产品、工业控制类产品、系统软件、支撑系统等。支持资产指纹规则 260000 条。 3. 协议识别：支持对检查目标全网协议进行识别，包括有 TCP/IP、IPX/SPX、NetBEUI、HTTP、FTP、工控协议（CoDeSys、GE-SRTP、SIEMENS、MELSEC-Q、omron 等）。 4. 不限操作客户端系统类型，无需安装任何客户端插件，使用 H5 即可直接运维 windows、Linux、网络设备等资源； 5. 威胁持续监测：提供 7*24H 全天候全资产的安全威胁监测服务，持续监测网络安全状态并及时进行分析与预警，包括高级可持续威胁（APT）攻击事件、高级黑客攻击事件、病毒事件（包括勒索病毒、蠕虫病毒、挖矿病毒、感染型病毒、后门型病毒、木马型病毒、破坏型病毒等）、木马事件（窃密木马、远控木马等）、僵尸网络事件、有害程序类事件（恶意广告、黑市工具、流氓推广等）、网络攻击事件	套	1

		（包括 SQL 注入、XML 注入、代码执行、权限绕过、跨站脚本攻击、命令执行等）、后门程序事件等。 6. 主动响应分析：分析人员综合所发现的安全事件、攻击情况，综合评价整体网络安全态势，包括告警趋势分析、威胁类型分布分析、高威胁攻击者分析等，并每月主动进行场景化安全分析，包括 APT 告警分析、恶意软件情况分析、网络攻击情况分析、WebShell 情况分析、内网安全情况分析、数据库安全情况分析、爆破行为分析、弱口令分析等。 7. 安全事件响应：安全托管运营团队对监测发现的安全隐患及事件按要求进行实时通告，同时根据用户需求每日同步安全情况。建立安全监测分析群实时推送封禁信息，包括高频攻击源、恶意软件 IOC、内外交互的恶意链接等，迅速抑制网络攻击。 8. 安全事件应急响应：在遇到网络安全攻击时，第一时间予以远程响应，协助采取紧急措施、将业务恢复到正常服务状态，并调查、分析安全事件入侵路径及原因，提供加固及整改建议防止再次被黑客“原路”攻击。 9. 运营汇报：建立微信工作群，实时推送封禁信息，包括高频攻击源、恶意软件 IOC、内外交互的恶意链接等，对于具备防护产品的场景，可进行联动封禁，阻止进一步攻击；安排服务专家在线进行运营情况汇报，进行威胁分析情况解读，并进行疑难解答。 10. ★增值服务：配合甲方完成安全防范管控梳理工作，包括安全监控视频、重大设备灾害防治、监测感知数据信息、风险评估报告、风险监测预警信息等。		
13	安全监测威胁情报系统	1. 支持域名威胁分析查询，查询结果应包括开源情报、TTP 情报、关联样本、可视化分析等；支持 IP 的威胁分析查询，查询结果应包括开源情报、TTP 情报、关联样本、可视化分析等； 2. 支持用户手动录入情报，对应格式应包含 IP、域名、URL、SHA1、MD5 等。录入内容字段应包括恶意类型、可信度、风险等级、威胁名称、情报来源、参考链接、威胁描述等； 3. 支持针对接入的情报源进行置信度标记、置信度展示、状态显示、情报源启停等功能。 4. 支持本地失陷主机情报库，用于检测内网失陷主机，支持勒索、挖矿、蠕虫、僵尸网络、木马后门、APT 攻击所控制系统，本地失陷主机情报数量 1000 万条并且精准度达到 99.99%； 5. 系统查询结果包括告警名称、最早发现时间、威胁类型、恶意家族、攻击链阶段、攻击团伙、置信度、当前状态、IOC 类型、恶意类型、影响平台、风险等级、是否定向攻击等信息； 6. 支持 APT 情报信息，包含 APT 攻击事件、勒索软件、蠕虫木马、黑客工具、僵尸网络、后门软件等关键威胁。 7. 支持对 SQL 注入、跨脚本攻击、grant 语句进行提权行为的审计，对审计记录返回内容中的敏感数据能进行隐秘处理，防止二次泄露。 8. 支持 B/S 架构 Http 应用三层审计，可提取包括应用系统的人员工号（账号）的身份信息，精确定位到人，并可获取 XML 返回结果。支持 C/S 架构 COM、COM+、DCOM 组件的三层审计，可提取应用层工号（账号）的身份信息，精确定位到人；支持框架：tomcat、apache、weblogic、jboss 9. 支持对 HTTP、FTP、TELNET、SMTP、POP3、NFS 协议的审计。 10. ★增值服务：配合甲方进行数据信息维护，基本信息中各分项进行处理，包括基础信息、证照信息、信息及监控系统、应急管理基本信息、应急预案基本信息、专业	套	1

		技术人员统计、应急培训演练统计、职业健康管理；		
14	机房集成服务	提供包含城市部件事件库、地理编码库、地形数据库等基础资源数据库和完成发现问题、派遣任务、问题处理、结果反馈、监督评价等各个环节的数字城管系统的集成服务	项	1
15	机房维保服务	提供机房设备维护及设备安全日志维护服务，每日针对异常流量、攻击日志进行分析并形成报告。	项	1

2、线路及机房托管服务清单

序号	项目	内容
1	服务器机房到指挥大厅 1000M 光纤	满足长葛市数字化城市管理中心数据传输访问带宽需求
2	服务器机房到政务网 1000M 光纤	满足长葛市数字化城市管理中心与相关责任单位数据传输访问带宽需求
3	公安视频与中心机房 1000M 光纤	满足长葛市数字化城市管理中心访问公安系统视频专网带宽需求
4	50 路高清监控到中心机房 100M 光纤	满足 50 个监控站点将视频影像传输到管理中心带宽需求
5	呼叫链路	满足呼叫中心 12319 网络热线需求
6	视频采集车无线网络	满足视频采集车传输视频影像到长葛市数字化城市管理中心的无线网络
7	机房托管服务	包含：服务器、交换机、路由器、存储、防火墙、机房和车载 UPS 电源、操作系统、防病毒系统等多台设备
8	机房数据异地云灾备	满足不少于 3T 或一个月数据异地云灾备部署支持完全备份、差异备份、增量备份、日志备份、数据异地容灾、CDP、数据零丢失、数据同步等多种容灾方式
9	视频监控点位维修保障	50 路室外型高清监控系统包含的所有设备维保和更换

10	手持终端使用费	无线信息采集城管通终端 80 部
11	手持终端信息流量费用	提供音视频信息传递服务
12	值班坐席终端设备服务	人工坐席 30 台电脑 5 台打印机的维修服务

附件 2：**网络与信息安全协议书**

网络与信息安全协议书

甲方应按照《中华人民共和国网络安全法》等法律法规的要求，履行相关网络安全义务，承担网络安全责任。

第一条 甲方承诺不利用乙方提供的服务及设备设施进行下列任何活动或发布、传播下列任何信息：

（1）从事危害国家安全、泄露国家秘密等犯罪活动；从事国家法律、法规、政策所禁止的活动或违背公共道德的活动；

（2）散布谣言，扰乱社会秩序，破坏社会稳定；散布垃圾邮件、病毒程序；黑客行为；侵权行为；博彩、赌博游戏等；

（3）危害国家安全、泄露国家机密、颠覆国家政权、破坏国家统一的信息；损害国家荣誉和利益的信息；煽动民族仇恨、民族歧视、破坏民族团结的信息；违反国家宗教政策的信息；宣扬邪教和封建迷信的信息；淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的信息；侮辱或者诽谤他人，侵害他人合法权益的信息；妨碍互联网运行安全的信息；其他有损于社会秩序、社会治安、公共道德的信息或内容；

（4）发布、传播其他违反国家法律、法规、政策内容的。

甲方同时承诺不为他人从事上述活动或发布、传播上述信息提供任何便利，如因甲方违反上述约定产生的一切责任和后果均由甲方承担。甲方认可乙方有权判断本协议项下甲方从事的活动或甲方发布的信息是否违法、违规或违反本协议有关规定，且乙方有权在提前通知甲方的情况下采取一切必要措施，包括但不限于暂停或终止提供本协议项下的服务、要求甲方进行整改等，但乙方上述权利不应被视为乙方有审核甲方行为或信息内容的义务或保证其合法合规的任何责任。

第二条 甲方不得有下列危害电信网络安全和信息安全的行为：

（1）对电信网络的功能或者存储、处理、传输的数据和应用程序进行违法删除或者修改。

（2）利用电信网络从事窃取或者破坏他人信息、损害他人合法权益的活动。

（3）故意制作、复制、传播计算机病毒或者以其他方式攻击他人电信网络等电信设施。

（4）危害电信网络安全和信息安全的其他行为。

若甲方存在上述任一情形的，乙方有权按相关规定暂停或停止提供服务、断开网络接入，保存有关记录，并向政府主管部门报告，由此引起的一切后果和责任由甲方负责。同时，乙方有权终止合同，并不承担任何责任。

第三条 甲方不得将接入设备转借或租赁给其它单位和个人使用，以防止非法信息的传播；否则，由其承担相关责任，乙方有权立即停止相关服务。

第四条 甲方应承担如下管理责任:

(1) 向所属员工或使用者宣传国家及电信主管部门有关电信安全的法规规定。

(2) 建立健全使用者档案，加强对使用者的管理、教育工作。

(3) 有健全的网络安全保密管理办法。

第五条 甲方有责任对其自身系统的网络安全状况负责，并定期对其系统的安全状况进行检查，若发生网络攻击、信息泄露等网络安全事件，乙方不承担相关责任。

第六条 甲方侧数据由甲方负责，如出现信息泄露、信息篡改等安全事件，乙方不承担责任。

第七条 甲方承诺采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。不得从事以下行为:

(1) 利用自己或他人的机器设备，未经他人允许，通过非法手段取得他人机器设备的控制权;

(2) 非授权访问、窃取、篡改、滥用他人机器设备上的信息，对他人机器设备功能进行删除、修改或者增加;

(3) 向其他机器设备发送大量信息包，干扰其他机器设备的正常运行甚至无法工作;或引起网络流量大幅度增加，造成网络拥塞，而损害他人利益的行为;

(4) 资源被利用进行网络攻击的行为或由于机器设备被计算机病毒侵染而造成攻击等一切攻击行为。

(5) 有意通过互联网络传播计算机病毒;

(6) 因感染计算机病毒进而影响网络和其它客户正常使用的行为。

第八条 甲方业务如使用乙方提供的 IP 地址，甲方需承诺并确认：甲方所提交的所有备案信息真实有效，且备案信息不得出现乙方任何内容。当提供的备案信息发生变化时应及时到备案系统中提交更新信息，如因未及时更新而导致备案信息不准确，乙方有权依法采取停止提供服务、断开网络接入等关闭处理措施。如因甲方原因造成信息未及时通知，引发相关网络信息安全事件的，由甲方自行承担相关责任。

甲方

签字盖章:

年 月 日

乙方（联合体牵头人）

签字盖章:

乙方（联合体成员）

签字盖章: